CLAIMS

What is claimed is:

1. A computer-implemented method for gathering security event data and rendering result data in a manageable format comprising the steps of:

creating scope criteria for analyzing security event data;

collecting the security event data from a plurality of security devices located at a first location;

storing the collected security event data at a second location;

analyzing the collected security event data with the scope criteria to produce result data, the result data accessible by a plurality of clients; and

rendering the result data in a manageable format for the plurality of clients.

2. The method of Claim 1, further comprising storing one or more of the scope criteria and the result data.

3. The method of Claim 1, wherein the first location is a distributed computing environment.

4. The method of Claim 1, wherein the second location is a database server.

5. The method of Claim 1, wherein the analyzing is performed at an application server to which the plurality of clients are coupled.

6. The method of Claim 1, further comprising searching the stored security event data for additional information identifying a security event.

7. The method of Claim 1, further comprising:
polling a database server for current stored security event data;
analyzing the current stored security event data to produce current result data; and
rendering the current result data.

8. The method of Claim 1, further comprising polling for messages containing information about scope criteria, security event data, or result data.

9. The method of Claim 1, further comprising pushing messages to a client wherein the messages contain information about scope criteria, security event data, or result data.

10. The method of Claim 1, wherein the step of rendering result data comprises presenting the result data in a chart format.

11. The method of Claim 1, wherein in response to analyzing the collected security event data, an action is executed.

12. The method of Claim 11, wherein the action is clearing security event data from storage.

13. The method of Claim 11, wherein the action is creating an incident from result data for preparing a response.

14. The method of Claim 1, wherein the step of collecting security event data further comprises converting the data to a uniform format.

15. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 1.

16. A method for managing security event data collected from a plurality of security devices comprising the steps of:

creating scope criteria for filtering security event data;

collecting security event data from a plurality of security devices located at a first location;

storing the collected security event data at a second location; and

applying the scope criteria to the collected security event data to produce a result, the result accessible by a plurality of clients.

17. The method of Claim 16, further comprising rendering the result in a rendering for output.

18. The method of Claim 16, wherein the first location is a distributed computing environment.

19. The method of Claim 16, wherein the second location is a database server.

20. The method of Claim 16, wherein the result is accessible by a plurality of clients coupled to a distributed computing environment.

21. The method of Claim 16, further comprising storing one or more of the scope criteria, and the result.

22. The method of Claim 16, wherein in response to producing a result, an action is executed.

23. The method of Claim 22, wherein the action is clearing stored security event data.

24. The method of Claim 22, wherein the action is creating an incident from a result.

25. The method of Claim 16, further comprising applying the scope criteria to a plurality of results.

26. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 16.

27. A computer-implemented system for managing security event data collected from a plurality of security devices comprising:

a plurality of security devices operable for generating security event data;

a database server coupled to the security devices, the database server operable for collecting security event data from the security devices;

an application server coupled to the database server, the application server operable for analyzing the security event data; and

a client coupled to the application server, the client operable for receiving a rendering of the analyzed security event data.

28. The system of Claim 27, wherein the database server is further operable for storing the collected security event data and the analyzed security event data.

29. The system of Claim 27, wherein the application server is further operable for creating an incident from the security event data for preparing a response.

30. The system of Claim 27, wherein the security devices are coupled to a distributed computing network.